חישוביות - תרגול 9

דוד קלוטה

2 ביוני 2026

מה נעשה היום?

1. מוודא פולינומי
2. $\mathrm{U}{-}s,t{-}\mathrm{HAMPATH}$ היא NP־שלמה
3. $3-\mathrm{COLORING}$ היא NP־שלמה
4. $2\mathrm{SAT} \in \mathrm{P}$

התחלנו!

9.1 מוודא פולינומי

תזכורת:

$$\mathrm{NP} \overset{\text{def}}{=\!=} \bigcup_{k\in\mathbb{N}_0} \mathrm{NTime}(n^k)$$

הגדרה 9.1.1 (מוודא פולינומי)**.** מוודא פולינומי לשפה L הוא מכונת טיורינג דטרמיניסטית V שמקבלת $x=(w,c)$ כך ש־c פולינומי ב־$|w|$, רצה בזמן פולינומי ב־$|w|$ ו־

$$\begin{aligned} \forall w \in L \quad & \exists c \in \Sigma^* : \quad V(w,c) = q_{\mathrm{acc}} \\ \forall w \notin L \quad & \forall c \in \Sigma^* : \quad V(w,c) = q_{\mathrm{rej}} \end{aligned}$$

משפט 9.1.1. *שפה L ניתנת לזיהוי בזמן פולינומי על ידי מכונת טיורינג אי־דטרמיניסטית $L \in \mathrm{NP}$ אמ״ם קיים מוודא פולינומי ל־L.*

9.2 $\mathrm{U}{-}s,t{-}\mathrm{HAMPATH}$ היא NP־שלמה

הגדרה 9.2.1. נגדיר את השפה $\mathrm{U}{-}s,t{-}\mathrm{HAMPATH}$ להיות:

$$\mathrm{U}{-}s,t{-}\mathrm{HAMPATH} \overset{\text{def}}{=\!=} \left\{ \langle G,s,t\rangle \;\middle|\; \begin{array}{l} G \text{ is an undirected graph} \\ \text{which contains a Hamiltonian path from } s \text{ to } t \end{array} \right\}$$

טענה 9.2.1. $\mathrm{U}{-}s,t{-}\mathrm{HAMPATH}$ *היא* NP־*שלמה.*

הוכחה. נוכיח זאת עם שתי טענות עזר:

טענת עזר 9.2.1. $\mathrm{U}{-}s,t{-}\mathrm{HAMPATH} \in \mathrm{NP}$.

הוכחה. נבצע הוכחה זאת על ידי בניית מוודא פולינומיאלי לשפה:

Algorithm 1 Polynomial-time verifier for $\mathrm{U}{-}s,t{-}\mathrm{HAMPATH}$

Require: $x = (w, c)$
Require: $w = \langle G, s, t\rangle$
Require: $G = (V, E)$
Require: $c = \langle v_1, \ldots, v_n\rangle$
if c does not have $|V|$ vertices **then**
    return False
end if
Let $i \leftarrow 1$
while $i \leqslant n$ **do**
    if v_i was seen before **then**
        return False
    end if
    $i \leftarrow i + 1$
end while
return $v_1 = s \wedge v_n = t$

נראה שהמוודא פולינומיאלי: ראשית, זמן הריצה הוא פולינומיאלי כי הבדיקות שהמוודא עושה הן פולינומיאליות בכמות הקודקודים והקשתות ושורה 1 מכריחה את c להיות פולינומיאלי ב־$|w|$.

נוכיח נכונות: אם $w \in \mathrm{U}{-}s,t{-}\mathrm{HAMPATH}$, אז קיים מסלול המילטוני ב־G מ־s ל־t. נסמנו $s, v_1, \ldots, v_n$ והמוודא יקבל. אם $w \notin \mathrm{U}{-}s,t{-}\mathrm{HAMPATH}$ אז אין מסלול המילטוני ולכן לא משנה מה c הבדיקות יכשלו והמוודא לא יקבל. □

טענת עזר 9.2.2. $\mathrm{U}{-}s,t{-}\mathrm{HAMPATH}$ *היא* NP־*קשה.*

הוכחה. נוכיח זאת באמצעות יצירת רדוקציה של $\mathrm{D}{-}s,t{-}\mathrm{HAMPATH}$ לבעיה זו. נגדיר פונקציה f לכל $G = (V, E)$ ו־$s, t \in V$ להיות

$$f(\langle G, s, t\rangle) = \langle G', s', t'\rangle$$

כך שבגרף המכוון G קיים מסלול המילטוני מ־s ל־t אמ"ם קיים בגרף הלא מכוון G' מסלול המילטוני מ־s' ל־t'.

יהיו בעבור כל קודקוד $v \in V$ הקודקודים $v_{\text{in}}, v_{\text{mid}}, v_{\text{out}}$. נסמן כעת

$$V' \stackrel{\text{def}}{=\!=} \bigcup_{v \in V} \{v_{\text{in}}, v_{\text{mid}}, v_{\text{out}}\}$$

נגדיר את קבוצת הצלעות להיות

$$E' \stackrel{\text{def}}{=\!=} \bigcup_{v \in V} \{(v_{\text{in}}, v_{\text{mid}}), (v_{\text{mid}}, v_{\text{out}})\} \cup \bigcup_{(u,v) \in E} \{(u_{\text{out}}, v_{\text{in}})\}$$

לבסוף, נסמן $G' = (V', E')$ ו־$s' = s_{\text{in}}, t't_{\text{out}}$.

בנייה זו אכן חשיבה בזמן פולינומי: על כל קודקוד ב־V אנו יוצרים 3 קודקודים בגרף החדש - פעולה בסדר גודל לינארי. כמו כן, יש לנו לא יותר מפי 3 צלעות, חסם לינארי גם כן. מכאן, הגודל פולינומי ב־$|\langle G\rangle|$ וכל הפעולות נעשות בזמן פולינומי אף הן.

נוכיח נכונות:

כיוון $\Longleftarrow$ נסמן את המסלול ההמילטוני ב־$s, v_1, \ldots, v_n, t$. אזי המסלול

$$s_{\text{in}}, s_{\text{mid}}, s_{\text{out}}, v_{1\text{in}}, v_{1\text{mid}}, v_{1\text{out}}, \ldots, v_{n\text{in}}, v_{n\text{mid}}, v_{n\text{out}}, t_{\text{in}}, t_{\text{mid}}, t_{\text{out}} \tag{1}$$

הוא מסלול המילטוני חוקי ב־G'.

כיוון $\Longrightarrow$ אם נראה שהמסלול ההמילטוני ב־G' הוא (1) אז נוכל פשוט לקחת את המסלול $s, v_1, \ldots, v_n, t$ ב־G ולקבל שהוא מסלול המילטוני. נראה שהוא אכן חייב להיראות מהצורה הזו, ובפרט שאין במסלול ההמילטוני מעבר מהצורה $(u_{\text{in}}, v_{\text{out}})$. נניח בשלילה שקיים מעבר כזה, ונניח כי $(u_{\text{in}}, v_{\text{out}})$ הוא הפעם הראשונה שהמעבר קורה. נניח שכבר ביקרנו ב־u_{mid} אבל ממי עברנו ל־u_{out}? מ־x_{in} אחר. כלומר, כבר עשינו $(x_{\text{in}}, u_{\text{out}})$ בסתירה לכך ש־$(u_{\text{in}}, v_{\text{out}})$ היה הפעם הראשונה בה זה קרה. אם עדיין לא ביקרנו ב־u_{mid}, כאשר נגיע אליו, זה יהיה בהכרח מ־u_{out} אבל אז ניתקע בו, בסתירה לכך ש־$t' = t_{\text{out}}$. □

נפעיל את שתי טענות העזר, וסיימנו. □

9.3 $3-\text{COLORING}$ היא NP־שלמה

הגדרה 9.3.1 (k־צביעה)**.** יהי $G=(V,E)$ גרף. k־צביעה של G היא פונקציה $A:V\to\{c_1,\dots,c_k\}$. נאמר ש־G k־צביע אם קיימת k־צביעה כך שאם $(u,v)\in E$ אז $A(u)\neq A(v)$

הגדרה 9.3.2 (השפה $3-\text{COLORING}$)**.** נגדיר את השפה $3-\text{COLORING}$ להיות

$$3-\text{COLORING}\overset{\text{def}}{=\!=}\{\langle G\rangle \mid G \text{ is 3-colorable}\}$$

טענה 9.3.1. $3-\text{COLORING}$ *היא* NP־*שלמה.*

הוכחה. על מנת להוכיח את הטענה, נידרש לשתי טענות עזר:

טענת עזר 9.3.1. $3-\text{COLORING}\in\text{NP}$.

הוכחה. נבנה מוודא פולינומי עבור $3-\text{COLORING}$:

Algorithm 2 Polynomial-time verifier for $3-\text{COLORING}$

Require: $x=\langle w,c\rangle$
Require: $w=\langle G\rangle$
Require: $G=(V,E)$
Require: c is a 3-coloring.

```
if c does not describe a coloring of |V| vertices then
    return False
end if
for each pair (u, v) ⊆ V where u ≠ v do
    if c(u) has more than one value ∨ c(v) has more than one value then
        return False
    end if
    if (u, v) ∈ E ∧ c(u) = c(v) then
        return False
    end if
end forreturn True
```

תרגיל 9.3.1. רשמו ניתוח זמן ריצה והוכחת נכונות.

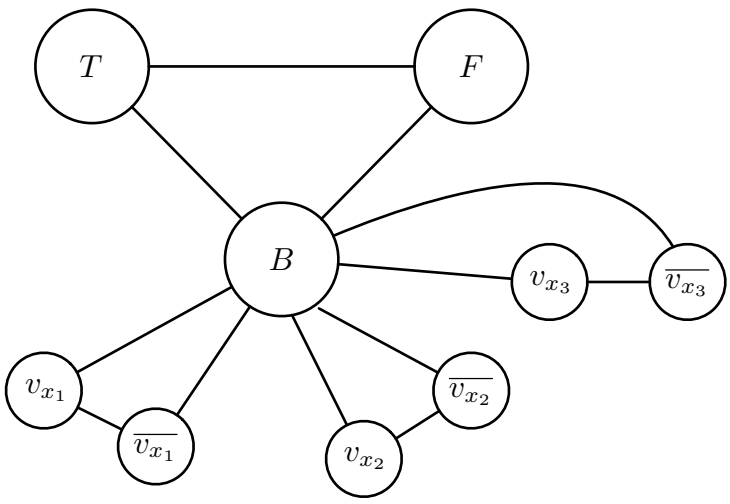
ו־$3-\text{COLORING}$ אכן ב־NP. □

טענת עזר 9.3.2. $3-\text{COLORING}$ *היא* NP־*קשה.*

הוכחה. נרשום רדוקציה מ־3SAT ל־$3-\text{COLORING}$ץ לכל נוסחת CNF ϕ נגדיר את f להיות

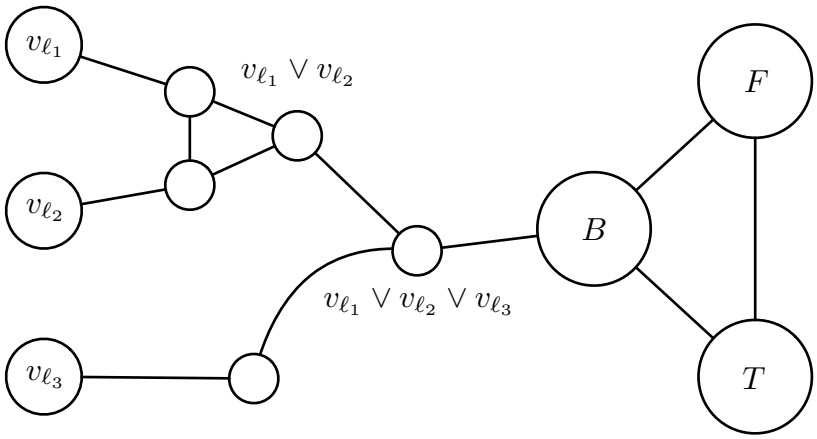
$$f(\langle\phi\rangle)=\langle G\rangle$$

כך ש־ϕ ספיקה אמ"ם G 3־צביעה.
נבנה את G באופן הבא:



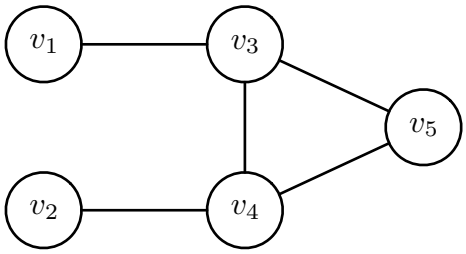
איור 1

נשים לב ש־B,T,F חייבים להיות צבועים בצבעים שונים. נזהה את הצבע של T עם ירוק, F עם אדום ו־B עם כחול. לכל משתנה $x_i \in \phi$ נבנה שני קודקודים $v_{x_i}, \overline{v_{x_i}}$, נחבר ביניהם ונחבר אותם ל־B. זה מכריח כל קודקוד לצבוע את v_{x_i} בירוק ואת $\overline{v_{x_i}}$ באדום או להפך. לכל פסוקית $c_j \ell_1 \vee \ell_2 \vee \ell_3$ נבנה את שרשרת הקודקודים הבאה:



איור 2

טענת עזר 9.3.3. *נתבונן בגרף*



איור 3

אם v_1, v_2 אדומים אז v_5 גם אדום. אם אחד מהם לא אדום אז v_5 לא יכול להיות ירוק.

מסקנה **9.3.1.** בשרשרת הקודקודים שמתאימה לפסוקית, אם $v_{\ell_1}, v_{\ell_2}, v_{\ell_3}$ אדומים אז גם $v_{\ell_1} \vee v_{\ell_2} \vee v_{\ell_3}$ אדום. אם אחד מהם לא אדום, אזי $v_{\ell_1} \vee v_{\ell_2} \vee v_{\ell_3}$ לא יכול להיות ירוק.

מאוד פשוט להוכיח חשיבות: גודל הגרף פולינומי בגודל ϕ כל לכל משתנה הוספנו שני קודקודים ולכל פסוקית עד 10 קודקודים. נוכיח כעת נכונות:

כיוון $\Longleftarrow$ נניח כי $\phi \in 3\text{SAT}$. לכן קיימת השמה $A : \{x_i\}_{i\in\mathbb{N}} \to \{\text{True}, \text{False}\}$ שמספקת את ϕ. נגדיר צביעה באופן הבא:

$$A'(v_{x_i}) = \begin{cases} \text{Green} & A(x_i) \\ \text{Red} & \neg A(x_i) \end{cases}$$

ונרחיב את הצביעה גם ל־v_{x_i}.

נשים לב שאת $v_{x_i}, \overline{v_{x_i}}$ צבענו באופן חוקי: לכל פסוקית $c_j = \ell_1 \vee \ell_2 \vee \ell_3$ נצבע את $v_{\ell_1} \vee v_{\ell_2} \vee v_{\ell_3}$ בירוק. זה חוקי כי ϕ ספיקה ולכן כל c_j מסופקת על ידי A ולכן קיים $\ell_i \in c_j$ המקיים $A(\ell_i) = \text{True}$. לכן, $A'(v_{\ell_i}) = \text{Green}$. מטענת עזר 9.3.3 זה אומר שניתן לצבוע את ℓ_1, ℓ_2, ℓ_3 בירוק.

כיוון $\Longrightarrow$ נניח ש־$\langle G \rangle \in 3-\text{COLORING}$ ונניח כי A' היא הצביעה. נגדיר השמה ל־ϕ על ידי

$$A(x_i) = \begin{cases} \text{True} & A'(v_{x_i}) = \text{Green} \\ \text{False} & A'(v_{x_i}) = \text{Red} \end{cases}$$

נניח בשלילה ש־A לא מספקת את ϕ. אז קיימת פסוקית $c_j = \ell_1 \vee \ell_2 \vee \ell_3$ לא מספקת, כלומר לכל $i \in [3]$ מתקיים כי $A'(v_{\ell_i}) = \text{Red}$. אבל אז ממסקנה 9.3.1 נקבל ש־$A'(v_{\ell_1} \vee v_{\ell_2} \vee v_{\ell_3}) = \text{Red}$ בסתירה לכך שהוא מחובר ל־F. □

נפעיל את שתי טענות העזר, וסיימנו. □